EXECUTIVE SECRETARIAT

ROUTING SLIP

TO:		ACTION	INFO	DATE	INITIAL
1	DCI				
2	DDCI		X		
3	EXDIR		X		
4	D/ICS		X		
5	DDI		X		
6	DDA		X		
7	DDO				
8	DDS&T		X		
9	Chm/NIC				
10	GC				
11	IG				
12	Compt				
13	D/OLL				
14	D/PAO				
15	VC/NIC		X		
16	NIO/S&T		X		
17	C/TTIC		X		
18					
19					
20					
21					
22					
	SUSPENSE		Date		

Remarks

[redacted]

Executive Secretary

15 Aug 85

Date

3637 (10-81)

25X1

8523964

United States Department of State

Washington, D.C. 20520

~~UNCLASSIFIED~~
~~with SECRET Attachment~~

August 14, 1985

Executive Registry
85- 207/3

Senior Interagency Group No. 23

TO: ~~CIA~~ - [redacted] STAT
Commerce - Mrs. Helen Robbins
Defense - COL David Brown
Energy - Mr. William Vitale
FBI - Mr. James Geer
Justice - Mr. Stephen Galebach
NASA - Mr. Kenneth Pedersen
NSA - [redacted] STAT
OMB - Mr. Alton Keel
OSTP - Dr. George Keyworth
NSC - Mr. William Martin
NSF - Dr. Bodo Bartocha

SUBJECT: SIG/TT Executive Committee Meeting

Attached is the Summary of Conclusions for the Executive Committee meeting of the SIG on domestic safeguards on supercomputers, held on August 12, 1985.

Ronald Lang
for Nicholas Platt
Executive Secretary

Attachments:
1. Summary of Conclusions.
2. List of Participants.

~~UNCLASSIFIED~~
~~With SECRET Attachment~~

DCI EXEC REG

B-223B

United States Department of State

Washington, D.C. 20520

August 13, 1985

SECRET

PARTICIPANTS: See Attached List

DATE AND TIME: Monday, August 12, 1985 at 3:00 p.m.

PLACE: Room 1105, Department of State

SUBJECT: Domestic Safeguards for Supercomputers

SUMMARY OF CONCLUSIONS

Under Secretary Schneider convened the Executive Committee of the SIG to reach an agreed interagency position on U.S. policy regarding domestic safeguards for supercomputers. The Under Secretary opened the meeting by underscoring the reasons for U.S. concern about uncontrolled access to supercomputers. He reviewed for the group the existing international regime that prohibits access for COCOM proscribed nationals. Mr. Schneider noted that the Japanese have been particularly vigorous in enforcing domestic safeguards; they have already denied 3 dozen visa applications on this basis. He added that if we are to maintain the safeguard agreements contained in the existing international regime, we must design and implement a US regime that is the functional equivalent of the international regime.

The following is a summary of issues discussed by the SIG Executive Committee:

Issue I: Category I - USG Owned and Operated Supercomputers: Should the U.S. Government apply a strict "no access" rule to supercomputers owned and operated by U.S. Government Agencies?

All USG agencies with the exception of DOE and OSTP agreed that USG owned and operated machines should have a strict "no access" rule applied to COCOM proscribed nations. OSTP and DOE indicated that they had not been briefed on the national security threat of COCOM proscribed national's use of the machine, and felt that the facts for restricting access were not well developed. However, it was stated that DOE was an active participant in the conceptualization and negotiation of the US-Japanese supercomputer agreement.

SECRET
DECLASS:OADR

NSA offered to provide a briefing for OSTP and DOE. OSTP and DOE said that they were planning a trip to Los Alamos at the end of next week, and would be briefed there as well. OSTP and DOE asked the group to reserve judgment on the issue until they returned from Los Alamos. The Chairman agreed.

Issue II: Category II - Privately Owned & Operated Supercomputers - The U.S. Government should restrict and/or deny access to COCOM proscribed nationals to universities and private sector supercomputers through:

Option 1: No access (accomplished through the visa process as a first step);

Option 2: No access with some limited exceptions (enforced by a combination of the visa process and a procedure for the US Government to grant exceptions); or

Option 3: Indirect access (through a monitoring process enforced by the supercomputer managers.

The issue of treatment of PRC nationals as a COCOM proscribed nation was raised by NSF. The group agreed that the PRC question could be dealt with in a manner consistent with COCOM guidelines.

After some discussion, the Under Secretary agreed that this issue should be considered along with that of Issue V -- consultations with the academic community. It was agreed that a team, led by the State Department and including all those involved in the international negotiations (plus NSF), would visit several universities to consult with the academic community on this question. The baseline proposal presented to thelacademic community would be the "no access" policy, with a view towards entering into a dialogue with them. He said that the SIG/TT would revisit this issue in September after the team visits.

Issue III: Should NSF funded and controlled supercomputer centers be treated as US Govenment owned and operated computers (regime discussed in Issue I) or as private computers (regime discussed in Issue II)?

Under Secretary Schneider said that the Supercomputer Working Group recommended that these machines be placed in the second category. NSF agreed, and the group concurred.

Issue IV: Voluntary Guidelines for Physical Security on Supercomputer Facilities.

NSF said that they found all of the guidelines in the options memo satisfactory with the exception of the security measures on remote terminals. This was impracticable given sheer numbers. NSF suggested that better security should be put in front end computers. The group accepted all other guidelines, and asked the Supercomputer Working Group to re-think the remote terminal issue.

Issue V: Consultations with the Academic Community

The group decided this issue in the context of Issue II.

SIG TT - Supercomputers
Monday, August 12, 1985
3:00 p.m., Room 1105

Name	Agency	Phone
William Schneider, Jr.	State	632-0410
[redacted]	CIA	[redacted]
[redacted]	CIA	[redacted]
[redacted]	DIA	[redacted]
Walter J. Olson	DOC	377-5491
Stephen Bryen	DOD	697-9347
George Menas	DOD	694-4625
Al Trivelpiece	DOE	252-5430
Carl Thorne	DOE:DP	252-2112
Don Ofte	DOE:DP	252-2179
Harry W. Porter	FBI	324-4646
Roger Diehl	FBI	324-4646
J. Michael Shepherd	Justice	633-4604
Rick Cinquegrara	Justice	633-5604
Douglas Norton	NASA	453-8458
[redacted]	NSA	[redacted]
[redacted]	NSA	[redacted]
David G. Wigg	NSC	395-5607
Erich Bloch	NSF	357-7748
Clifford Jacobs	NSF	357-9695
John Moore	NSF	357-9427
Arthur J. Kusinski	NSF	357-9445
Dan Taft	OMB	395-3285
Norine Noonan	OMB	395-3534
John McTague	OSTP	395-3961
Ora Smith	OSTP	395-5052
Michael Marks	State	632-8071
Pam Smith	State	632-8724
Sherwood McGinnis	State	632-0533
David Wilson	State	632-1421
Robert Price	State	632-0964
Dale Tahtinen	State:EB/ITC	632-1625
Jerry W. Leach	State:PM	632-5097
Ken Peoples	State:PM	632-1236
Ralph A. Hallenbeck	State:PM	632-0440
Dan Abbasi	State:PM/STA	632-5097

25X1
25X1
25X1
25X1
25X1
25X1
25X1

Wang 74

EXECUTIVE SECRETARIAT
ROUTING SLIP

TO:		ACTION	INFO	DATE	INITIAL
1	DCI				
2	DDCI		X		
3	EXDIR		X		
4	D/ICS				
5	DDI		X		
6	DDA				
7	DDO				
8	DDS&T				
9	Chm/NIC				
10	GC				
11	IG				
12	Compt				
13	D/OLL				
14	D/PAO				
15	VC/NIC	X			
16	NIO/S&T		X		
17	C/TTIC		X		
18	ER				
19					
20					
21					
22					
	SUSPENSE		Date		

Remarks

To 15: Per DDCI, Julian Nall will attend this mtg as the principal with [redacted] as the "plus-one". ES has called in the names. [redacted] 25X1

25X1

Executive Secretary

8 Aug 85

Date

3637 (10-81)

United States Department ~~of State~~

Washington, D.C. 20520

SECRET

August 7, 1985

Senior Interagency Group No. 23

TO:
CIA - [redacted] 25X1
Commerce - Mrs. Helen Robbins
Defense - COL David Brown
Energy - Mr. William Vitale
FBI - Mr. James Geer
Justice - Mr. Stephen Galebach
NASA - Mr. Kenneth Pedersen
NSA - [redacted] 25X1
OMB - Mr. Alton Keel
OSTP - Dr. George Keyworth
NSC - Mr. William Martin
NSF - Dr. Bodo Bartocha

SUBJECT: Announcement of a Meeting of the Executive Committee of the SIG on Transfer of Strategic Technology

The SIG/TT Executive Committee will meet on Monday, August 12, 1985, at 3:00 p.m. in Room 1105 at the State Department.

The issue for the meeting will be the question of domestic safeguards on supercomputers. Attached you will find an options paper which has been prepared by the Supercomputer Working Group.

Attendance is principal plus one. We respectfully request that only principals sit at the table. Please telephone the names of your participants to Jerry Leach (6325097) or Kristen Johnson (632-5104) by COB Friday, August 9.

Boorkmley

~~for~~ Nicholas Platt
Executive Secretary

Attachments:
- Policy Options Paper on Domestic Safeguards for Supercomputers

SECRET
DECL:OADR

B-223B

United States Department of State

Under Secretary of State for
Security Assistance, Science and Technology

Washington, D.C. 20520

August 6, 1985

SECRET
MEMORANDUM

TO: SIG Members Represented on the Supercomputer Working Group

FROM: William Schneider, Jr.

SUBJECT: SIG Executive Committee Meeting on Domestic Supercomputer Policy
Monday, August 12, 1985
Room 1105 - 3:00 p.m.

Over the last few months, the Supercomputer Working Group (SWG) has been meeting to discuss options for a domestic supercomputers safeguards policy that achieves "functional equivalency" with the international regime that is in place with Japan and the FRG.* Based on the work of the SWG, it is now necessary to make several policy decisions so that the we can proceed with a domestic safeguards program. For this reason, I am calling a SIG meeting for Monday, August 12, to focus on some of the available options that have been identified by the SWG.

I. National Security Concerns About Supercomputers

Supercomputers, though general purpose in nature, can be used for highly sensitive national security applications, e.g.; nuclear weapons design and testing, anti-submarine warfare, and will be critical to the development of the Strategic Defense Initiative, including directed-energy weapons. Consequently, the United States Government has placed special restrictions on the sale of supercomputers overseas under the authority of the Export Administration Act, prohibiting these very sophisticated machines from being sent to any COCOM proscribed country. These restrictions had the following goals:

1. To assure a supercomputer is not acquired by any COCOM proscribed country.

2. To assure that COCOM proscribed nationals will not have access to supercomputer production technology.

---

*The existance of this regime is not generally known, and should be treated as classified information.

3. To assure that COCOM proscribed nationals cannot access to or use of Western supercomputers in order to gain insight on supercomputer technology or to perform military or intelligence related work that could not be performed on a lesser machine.

There seems to be agreement that illigitimate use of U.S. supercomputers for production work on direct military or intelligence applications will be unlikely if COCOM proscribed nationals have reason to believe that work they might do will be monitored. Without some form of monitoring, however, they might risk supercomputer access where they were unable to do certain things of great military importance without a supercomputer, and the risk of detection was low. Due to the lack of any policy to the contrary, COCOM proscribed nation scientists in the past have been allowed hundreds of hours on U.S. supercomputers -- more than enough time, some contend, for significant work on things of immediate military or intelligence importance to have been done.

There are 109 U.S. origin supercomputers in the world (excluding the supercomputers at the Department of Defense), sixty-five of which are located in the United States. Of these sixty-five, six are located at U.S. universities and twenty-nine are located at U.S. Government installations. The remaining thirty are owned and operated by the private sector. Most of the private sector machines are used exclusively by the owner, but two of the private sector machines are time-leased to any customer. In addition to the installed supercomputers, the National Science Foundation will fund four new supercomputer centers at Princeton, University of Illinois (Urbana Champaign), University of California (San Diego) and Cornell.

II. Policy Background

In a SIG meeting on March 16, 1984, it was decided that we would seek an agreement with the Japanese (the only other manufacturer of supercomputers) to prevent the utilization and acquisition of or access to supercomputer technology by COCOM proscribed nationals. It seemed to be futile to restrict access to supercomputers if COCOM proscribed nationals could gain substantial knowledge about supercomputers, or perhaps even run programs with military applications, through the use of supercomputers located outside their borders.

We were successful in our discussions with the Japanese. They agreed with us to condition foreign sales with a "no access for COCOM proscribed nationals" clause. It should be noted that under this agreed regime all exports

of supercomputers are conditioned with controls on access by all COCOM proscribed nationals. This includes PRC nationals. Nevertheless, because of the continuing liberalization in our relations with China, the SWG expects to revisit this issue for the purpose of whether to make any further recommendations to the SIG.

When asked about the lack of any domestic "no access" policy, U.S. negotiators responded that we had this matter under review, and planned to take some action in the near future. Furthermore, we told them that it was our intent to construct a national security package to deal with this problem, including both domestic and international elements.

At the last SIG meeting on May 8, we floated a draft national policy on use of or access to domestic supercomputers (Tab 1). Our view was that it made sense to restrict access to U.S. government owned machines first, and then to consider how to control COCOM proscribed access to other machines located in the U.S. It was pointed out that this was not as simple as it might appear, in that the National Science Foundation was funding new supercomputer centers at U.S. universities.

The SWG has discussed options for restricting access. The SWG believes that formal consultations with academia and the private sector will be helpful in formulating a USG policy, but feels that it needs further guidance of the SIG before it can speak with one voice in discussion options with these groups. The SWG has requested the SIG to decide what options should be selected for presentation during these consultations as the draft USG policy.

ISSUES FOR DECISION

Issue I:

Category I - - USG Owned & Operated Supercomputers

Should the U.S. Government apply a strict "no access" rule to supercomputers owned and operated by U.S. Government agencies?

Pros -- This would be a necessary step in conforming the international regime in place to the U.S. context and would be the minimum necessary to demonstrate our intent to deny access to COCOM proscribed nationals.

-- Without this minimum step, it will be difficult at best to maintain our partnership with Japan

and Germany concerning this issue and to continue to ensure that uniform safeguards are attached to all internal sales of supercomputers.

Cons -- There might be the desire on the part of U.S. Government Agencies to permit access to COCOM proscribed nationals for the release of unclassified information, in keeping with the intent of existing bilateral agreements.

-- When the academic community learns of a USG decision to uniquivically deny access to USG owned and operated supercomputers, they may regard this a prejudicial to the outcome ofthe regime that might apply to other supercomputers, including theirs.

Yes_____ No_____

Issue II:

Category II -- Privately Owned & Operated Supercomuters

The U.S. Government should restrict and/or deny access to COCOM proscribed nationals to universities and private sector supercomputers through:

Option 1 -- Strict "no access" by uses of the visa process through straight denials or amendments to the visa.

Pros -- This would conform with actions taken by the Japanese as a result of the international regime and would be totally consistent with conditions being placed on all international sales.

-- It would demonstrate our serious intent not to allow loopholes in our domestic safeguard system for supercomputers and serve as a role model for importing governments to follow.

-- This approach is consistent with the goals of our policy under the Export Administration Act.

-- This approach would provide the greatest screen of protection against COCOM proscribed access to U.S. supercomputers.

-- This approach would be enforced by the U.S. Government rather than the academic and

business communities and would not encumber them with the bureaucratic difficulties of a "indirect access" system (Option 3).

-- We expect that the approximate number of affected individuals would be small.

Cons -- It may stimulate new, tougher restrictions on U.S. scientists working in COCOM proscribed countries.

-- While it will certainly make access for COCOM proscribed operatives much more difficult, it may not be 100% effective.

-- A move to restrict access would effectively cut off a portion of our S&T cooperation with the COCOM proscribed nations. The policy would prevent their scientists from running programs on benign scientific projects.

-- Some in the academic community will regard this policy as a restriction on scientific and academic freedoms.

-- This approach will involve a greater effort by the INS and FBI to monitor the limited core group that might attempt to access supercomputers, especially through time sharing service center operations where the customer is less well known compared with situations existing in the university center.

Option 2 -- Option 1 (no access) with some exceptions, as determined by the USG, on a case-by-case basis.

Pros -- This would provide a general policy of "no access", while allowing some exceptions desirable to the academic community and agreed to by the U.S. Government.

Cons -- While presumably providing less access than in Option 3 below, this approach would have the same drawbacks as with Option 3 concerning its affect on the international regime.

-- The USG would become involved in reviewing of cases for approval, which could create bureaucratic strains for the USG as well as unhappiness in the academic and business communities.

-- Supercomputer centers would be encumbered with many of the same bureaucratic and enforcement requirements as in Option 3.

Option 3 -- Indirect Access for COCOM proscribed nationals for certain well defined cases. (A draft plan for such a regime is attached at Tab 2).

Pros -- Permits access for COCOM proscribed nationals working on basic scientific projects, with subject matter that presents no national security threat, and therefore permits the continuation of certain joint S&T work.

-- Through screening of COCOM proscribed nationals' programs, the academic/business community (and hopefully the USG) would have greater knowledge of program content.

-- Some sectors of the U.S. academic community may find this flexible policy more acceptable.

Cons -- Creates a very complicated bureaucratic structure through which access would be granted.

-- There would be a greater possibility of diversion for malicious use than with a "no access" policy.

-- Almost certainly would place the burden of access decisions and enforcement on the shoulders of the supercomputer center managers, which we assume would make them uncomfortable.

-- Supercomputer centers would have to deal with remote access to the supercomputer, which would make enforcement even more difficult.

-- If indirect access was readily available to COCOM proscibed nationals in the U.S., it would be impossible to continue to impose full restrictions on U.S. international sales.

Option 1: No access _____

Option 2: No access with some limited exceptions_____

Option 3: Indirect access_____

Issue III

Should NSF funded and controlled supercomputer centers be treated as US Government owned and operated computers (regime discussed in issue 1) or as private computers (regime discussed in issue 2).

The SWG recommends, in order to prevent dual systems of control for University Supercomputers Centers, that NSF affiliated machines be included within Category II, under whatever option is agreed to.

Category I _____ Category II _____

Issue IV

Regardless of what options are chosen, the SWG recommends certain immediately available minimal safeguards be applied by non-Government Agency owned Supercomputer Centers on a voluntary basis. This step is consistent with the international regime in place, and helps to bring us one step closer to a functional equivilant of the international regime. This would be accomplished through periodic USG briefings for all supercomputer owners and managers. The proposed measures include:

a. physical security of the computer, peripheral equipment, software, and on-site terminals;

b. physical security of all remote terminals; and

c. control of usage by means of passwords for all users, compartmented access categories and other procedures.

Yes_____ No_____

Issue V:

The SWG recommends that based on SIG guidance a small team led by State begin discussions with the academic community as soon as possible in order to come to an agreed domestic safeguard program.

Yes _____ No _____

NATIONAL POLICY FOR PROHIBITING ACCESS BY NON-RESIDENT ALIENS OF PROSCRIBED COUNTRIES TO U.S. GOVERNMENT OWNED OR CONTROLLED SUPERCOMPUTERS

SECTION I - SCOPE AND APPLICABILITY

1. This policy prohibits the acquisition, access or use of U.S. Government owned or controlled supercomputers by non-resident aliens of COCOM-proscribed and other proscribed nations. Supercomputers are extremely valuable tools in nuclear weapons design and testing, advanced aerodynamic and hydrodynamic research, the development of directed-energy weapons, and other militarily critical technologies. Such computers are known to be targeted by the Soviet military research and development community and by the Soviet Intelligence services.

SECTION II - POLICY

2. It is the policy of the Government of the United States that non-resident aliens of COCOM-proscribed and other proscribed nations be prohibited from acquiring, accessing or using U.S. Government owned or controlled supercomputers. To effect this policy, the following security measures should be implemented:

a. Computer center security against theft or unauthorized use of hardware and software;

b. Appropriate checks to ensure that access to the computer center will be limited to authorized persons;

c. Password or ID protocols for access by any user;

d. No passwords or IDs issued to any non-resident aliens of COCOM-proscribed or other proscribed nations;

e. No conscious or direct ties to the networks of COCOM-proscribed or other proscribed nations, or to networks whose subscribers include COCOM-proscribed or other proscribed nations; and

f. Appropriate monitoring of computer usage.

DRAFT

SECTION III - RESPONSIBILITIES

3. The heads of Federal departments, agencies and organizations are responsible for prohibiting the acquisition, access or use by non-resident aliens of COCOM-proscribed and other proscribed nations of supercomputers owned or controlled by such department, agency or organization.

4. The National Security Agency is responsible for maintaining a current list of those equipments classified as supercomputers.

5. The National Telecommunications and Information Systems Security Committee is responsible for the revision of this policy as necessary.

SECTION IV - DEFINITIONS

6. As used in this policy:

a. "Supercomputer" is defined as any computer whose processing data rate, storage capacity and performance are significantly superior to most existing equipment and which is classified as a supercomputer by the National Security Agency.

b. "Other proscribed nations" are defined as those nations as determined by the Secretary of State under Section 6 of the Export Administration Act of 1979 to be subject to export controls to the extent necessary to further the foreign policy of the United States or to fulfill its declared international obligations.

SECTION V - EXCEPTIONS

7. Nothing in this policy alters or contravens the provisions of existing policies or regulations which pertain to limitations placed on access to or the protection of Government owned or controlled automated information systems which generate, store, process, transfer or otherwise handle classified or sensitive, though unclassified, Government or Government-derived information.

8. Exceptions to this policy must be approved by the National Telecommunications and Information Systems Security Committee.

DRAFT

Guidelines for Domestic Supercomputers

Supercomputers, though general purpose in nature, have developed highly sensitive national security applications, e.g.; nuclear weapons design and testing, anti-submarine warfare, cryptography, and directed-energy weapons. Because of this, the Government has developed the following guidelines to protect against uses detrimental to national security interests in general, and in particular, by COCOM-proscribed nationals. This document presupposes that limited indirect access as described will not permit such use. These guidelines are designed to provide relatively little interference with legitimate use of supercomputers in academic and commercial environment.

The general policy of the United States Government is that COCOM-proscribed nationals, organizations, or their representatives should not have access to supercomputers. This policy is not to interfere in the legitimate usage of supercomputers by US citizens or other nationalities.

These guidelines were developed in consulation with the academic community and private sector, and provide guideance for the management of both publically and privately funded supercomputers.

I. Supercomputer Physical Security & Management

USG-funded supercomputer centers will be managed by individuals who have had a background investigation. The USG will offer background investigations to individual managers at other supercomputer centers.** The USG will brief supercomputer center managers on supercomputing security issues at startup and will maintain regular communication thereafter.

The supercomputing center management will be responsible for security at the centers to include (not exclusively):

a. physical security of the computer, peripheral equipment, software, and on-site terminals;

b. physical security of all remote terminals;

c. control of usage by means of passwords for all users, compartmented access categories and other procedures; and

---

**This program could be implemented with the cooperation of the supercomputer manufacturers.

d. routine security briefings for all operators and users.

II. Use of and Access to Supercomputers

As previously stated, it is the general policy of the USG to allow no access by COCOM-proscribed nationals to supercomputers. In order to permit scientific research in certain limited cases for COCOM-proscribed nationals, exceptions may be granted on a case-by-case basis provided several criteria are met in order to insure against uses that are detrimental to the national security.

COCOM-proscribed nationals may only be granted up to no. of hours ** by the supercomputer center manager. Permission for programs to be run will be based upon a detailed description of the proposed project to be completed by the proscribed national on a standardized application form. (This will be developed by the USG and the academic/business community.) The supercomputer center manager will have final approval authority for the program to be run, and their decision will be based upon the following guidelines and procedures:

1. The program to be run does not involve USG national security concerns, including but not limited to:

-cryptography

-nuclear weapons design

-advanced aerodynamics for aircraft and missiles

-hydrodynamics

-to be determined

These topics will be dicussed, reviewed and modified as necessary on a periodic basis by the USG Supercomputer Working Group.

2. There will be no access to the system-sensitive software, assembler, operating system source code, compiler source code, source code for optimized applications subroutines, etc.

** NSA Proposal: ten hours of time in any three month period

DRAFT

3. COCOM-proscribed nationals may not have any connect access to a supercomputer. Their source code must be written on a lesser machine, and any program de-bugging will be done on a lesser machine as well.

4. If access is permitted, the program shall be run by the supercomputer center management (i.e., no direct access).

5. If access has been denied and the supercomputer center manager believes that the case merits further review, the case may be referred for an advisory opinion by the US Supercomputer Working Group.

6. If access has been granted and it is believed that, subsequent to the run, the product raises national security concerns, the case will be referred to the Supercomputer Working Group for an advisory opinion.

7. The above procedures also apply to any remote terminal access to a supercomputer. The supercomputer center management will be responsible for providing guidance to its affiliated remote access sites, as well as for making the final determination concerning access and legitimacy of run results. The run must be done by the supercomputer center management; and these results would then be transferred to the remote access site..

8. Non-proscribed nationals will not provide concealed access for proscribed nationals; i.e., they will not do work for proscribed nationals in order to circumvent the limited exception procedure described above.

DRAFT

EXECUTIVE SECRETARIAT
ROUTING SLIP

TO:		ACTION	INFO	DATE	INITIAL
1	DCI		X		
2	DDCI				
3	EXDIR		X		
4	D/ICS				
5	DDI		X		
6	DDA				
7	DDO				
8	DDS&T				
9	Chm/NIC				
10	GC				
11	IG				
12	Compt				
13	D/Pers				
14	D/OLL				
15	D/PAO				
16	SA/IA				
17	AO/DCI				
18	C/IPD/OIS				
19	NIO /S&T		X		
20	C/TTIC		X		
21	VC/NIC	X			
22					
	SUSPENSE				

Date

Remarks

STAT Understand [redacted] is our principal and [redacted] the alternate.

25X1

25X1

[redacted]

Executive Secretary

2 May 85

Date

3637 (10-81)

S/S 8513352

United States Department of State

Washington, D.C. 20520

May 1, 1985

Executive Registry
85- 207/1

UNCLASSIFIED (With SECRET Attachment)

Senior Interagency Group No. 23

TO:

OVP	-	Mr. Donald P. Gregg
NSC	-	Mr. Robert Kimmitt
ACDA	-	Mr. William Staples
CIA	-	[redacted] STAT
Commerce	-	Mrs. Helen Robbins
Customs	-	Mr. Stephen Dougherty
Defense	-	COL R.J. Affourtit
Energy	-	Mr. William Vitale
FBI	-	Mr. Edward O'Malley
JCS	-	MAJ Michael Emerson
Justice	-	Mr. Stephen Galebach
NASA	-	Mr. Kenneth Pedersen
NSA	-	[redacted] 25X1
OMB	-	Mr. Alton Keel
OSTP	-	Dr. George Keyworth
Treasury	-	Mr. Edward Stucky
USTR	-	Amb. Michael Smith

SUBJECT: Announcement of the Meeting of the SIG on the Transfer of Strategic Technology, May 8, 1985

The SIG/TT will meet on Wednesday, May 8, at 2:30 p.m. in the Operations Center Conference Room (Room 7516) at the State Department.

Attendance is principal plus one. We respectfully request that only principals sit at the table.

Please telephone the names of your participants to Al O'Neill or Donna Wright (632-5099 or 5104) by noon Tuesday, May 7.

Nicholas Platt
Executive Secretary

Attachments:
-Agenda
-Domestic Supercomputer Policy

UNCLASSIFIED (With SECRET Attachment)

DCI EXEC REG

A-23B

SECRET

SENIOR INTERAGENCY GROUP ON TECHNOLOGY TRANSFER
Wednesday, May 8, 1985 at 2:30 p.m.

Operations Center Conference Room (7516)

I. Opening Statement

II. Items for Discussion and Decision

A. Follow-up on the 1985 COCOM HLM

B. Disclosure of Sensitive Information Through Unclassified Data Bases

C. NSDD on Technology Transfer

D. Supercomputers

(1) Domestic Policy
(2) Formal Designation of Working Group
(3) India and Supercomputers

E. Technology Transfer Through Space Programs

F. U.S. Policy Toward Telecommunications Sales to the PRC

G. Response to European Concerns Over West-West Technology Transfer Problems

H. Strategic Trade Officers Conference in Tokyo

III. Other Business

SECRET
DECL: OADR

NATIONAL POLICY FOR PROHIBITING ACCESS BY NON-RESIDENT ALIENS OF PROSCRIBED COUNTRIES TO U.S. GOVERNMENT OWNED OR CONTROLLED SUPERCOMPUTERS

SECTION I - SCOPE AND APPLICABILITY

1. This policy prohibits the acquisition, access or use of U.S. Government owned or controlled supercomputers by non-resident aliens or COCOM-proscribed and other proscribed nations. Supercomputers are extremely valuable tools in nuclear weapons design and testing, advanced aerodynamic and hydrodynamic research, the development of directed-energy weapons, and other militarily critical technologies. Such computers are known to be targeted by the Soviet military research and development community and by the Soviet Intelligence services.

SECTION II - POLICY

2. It is the policy of the Government of the United States that non-resident aliens of COCOM-proscribed and other proscribed nations be prohibited from acquiring, accessing or using U.S. Government owned or controlled supercomputers. To effect this policy, the following security measures should be implemented:

a. Computer center security against theft or unauthorized use of hardware and software;

b. Appropriate checks to ensure that access to the computer center will be limited to authorized persons;

c. Password or ID protocols for access by any user;

d. No passwords or IDs issued to any non-resident aliens of COCOM-proscribed or other proscribed nations;

e. No conscious or direct ties to the networks of COCOM-proscribed or other proscribed nations, or to networks whose subscribers include COCOM-proscribed or other proscribed nations; and

f. Appropriate monitoring of computer usage.

SECTION III - RESPONSIBILITIES

3. The heads of Federal departments, agencies and organizations are responsible for prohibiting the acquisition, access or use by non-resident aliens of COCOM-proscribed and other proscribed nations of supercomputers owned or controlled by such department, agency or organization.

4. The National Security Agency is responsible for maintaining a current list of those equipments classified as supercomputers.

5. The National Telecommunications and Information Systems Security Committee is responsible for the revision of this policy as necessary.

SECTION IV - DEFINITIONS

6. As used in this policy:

a. "Supercomputer" is defined as any computer whose processing data rate, storage capacity and performance are significantly superior to most existing equipment and which is classified as a supercomputer by the National Security Agency.

b. "Other proscribed nations" are defined as those nations as determined by the Secretary of State under Section 6 of the Export Administration Act of 1979 to be subject to export controls to the extent necessary to further the foreign policy of the United States or to fulfill its declared international obligations.

SECTION V - EXCEPTIONS

7. Nothing in this policy alters or contravens the provisions of existing policies or regulations which pertain to limitations placed on access to or the protection of Government owned or controlled automated information systems which generate, store, process, transfer or otherwise handle classified or sensitive, though unclassified, Government or Government-derived information.

8. Exceptions to this policy must be approved by the National Telecommunications and Information Systems Security Committee.

EXECUTIVE SECRETARIAT

ROUTING SLIP

TO:		ACTION	INFO	DATE	INITIAL
1	DCI				
2	DDCI		X		
3	EXDIR		X		
4	D/ICS				
5	DDI		X		
6	DDA				
7	DDO		X		
8	DDS&T				
9	Chm/NIC				
10	GC				
11	IG				
12	Compt				
13	D/Pers				
14	D/OLL				
15	D/PAO				
16	SA/IA				
17	AO/DCI				
18	C/IPD/OIS				
19	NIO/S&T		X		
20	C/TTIC		X		
21					
22					
	SUSPENSE _____ Date				

Remarks

25X1

Executive Secretary

13 Jan 65

Date

3637 (10-81)

C/H

S/S 8501440

United States Department of State

Washington, D.C. 20520

85-207

UNCLASSIFIED
(With SECRET Attachment)

January 17, 1985

Senior Interagency Group No. 23

TO :

OVP	-	Mr. Donald P. Gregg
NSC	-	Mr. Robert Kimmitt
ACDA	-	Mr. William Staples
CIA	-	[redacted] STAT
Commerce	-	Mrs. Helen Robbins
Customs	-	Mr. Stephen Dougherty
Defense	-	COL R.J. Affourtit
Energy	-	Mr. William Vitale
FBI	-	Mr. Edward O'Malley
JCS	-	LTC Thomas O'Connell
Justice	-	Mr. Ronald Blunt
NASA	-	Mr. Kenneth Pedersen
NSA	-	[redacted] STAT
OMB	-	Mr. Alton Keel
OSTP	-	Dr. George Keyworth
Treasury	-	Mr. Christopher Hicks
UNA	-	Amb. Harvey Feldman
USTR	-	Mr. Dennis Whitfield

SUBJECT: SIG/TT Executive Committee Meeting

Attached is the Summary of Conclusions for the Executive Committee meeting of the SIG on the Transfer of Strategic Technology, held on January 7, 1985.

Nicholas Platt
Executive Secretary

Attachment:
Summary of Conclusions

UNCLASSIFIED
(With SECRET Attachment)

DCI EXEC REG

B1173B

SECRET January 16, 1985

PARTICIPANTS: See Attached List

DATE AND TIME: January 7, 1985 at 10:00 a.m.

PLACE: Room 1206A, Department of State

SUBJECT: Resolution of the Belgian ITT Case on the Sale of a Fiber Optic Telephone Installation for Beijing

SUMMARY OF CONCLUSIONS

Under Secretary Schneider convened the Executive Committee of the SIG to reach an agreed interagency position on a Belgian case before COCOM. The case involves the proposed sale of a telephone network for Beijing by ITT's Belgian subsidiary BTM. The installation is to use short optical fiber links in place of conventional cable.

At the meeting, it was decided that the USG would remove its earlier condition in COCOM limiting the system's data rate to 34 megabits per second and agree to permit a rate of 140 megabits/sec.

As a result of the meeting and a follow-up working group session, it was decided that the USG would seek written agreement from the Belgian government on the following package of conditions:

--ITT must retain control of all spare parts and not transfer to the PRC any test equipment specific to 140 megabit pulse code modulation (PCM) equipment,

--The Chinese end-users must be identified by the time the installation work begins, (a condition previously accepted by the GOB)

--No regenerator or repeater equipment will be installed with the Beijing system, (a condition previously accepted by the GOB)

--There will be no transfer to the PRC of manufacturing technology.

On January 10, the Department cabled Embassy Brussels to seek Belgian agreement to the U.S. conditions. We are awaiting a Belgian response, which we expect will be positive.

SECRET
DECL: OADR

EXECUTIVE COMMITTEE MEETING
SIG ON THE TRANSFER OF STRATEGIC TECHNOLOGY

January 7, 1985

Room 1206A, Department of State

PARTICIPANTS

State	U/S William Schneider, Chairman Mr. Michael Marks, T Mr. Thomas Niles, EUR Mr. Robert Price, EB Mr. Stephen Schlaikjer, EAP/C
CIA	[redacted] STAT
Commerce	Mr. Vincent De Cain
NSA	[redacted] STAT
DOD	Mr. Stephen Bryen Mr. Dan Barney Mr. Michael Higgins LTC Nicholas P. Mihnovets